(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 304 830 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
23.04.2003 Bulletin 2003/17

(51) Int Cl.[7]: **H04L 12/24**, H04L 12/46

(21) Application number: **02102400.5**

(22) Date of filing: **01.10.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **05.10.2001 FI 20011949**
21.05.2002 US 151319

(71) Applicant: **Stonesoft Corporation**
00210 Helsinki (FI)

(72) Inventor: **Jalava, Mika**
02580 Siuntio (FI)

(74) Representative: **Äkräs, Tapio**
Kolster Oy Ab,
Iso Roobertinkatu 23
00120 Helsinki (FI)

(54) Virtual private network management

(57) The invention provides a centralized VPN management of a plurality of VPN sites by means of a VPN Information Provider (VIP) (400, 401). Management of a VPN device is distributed so that at least part of the VPN configuration is centrally managed without giving away control of the firewall rulebase or other critical local configuration used in the VPN device.

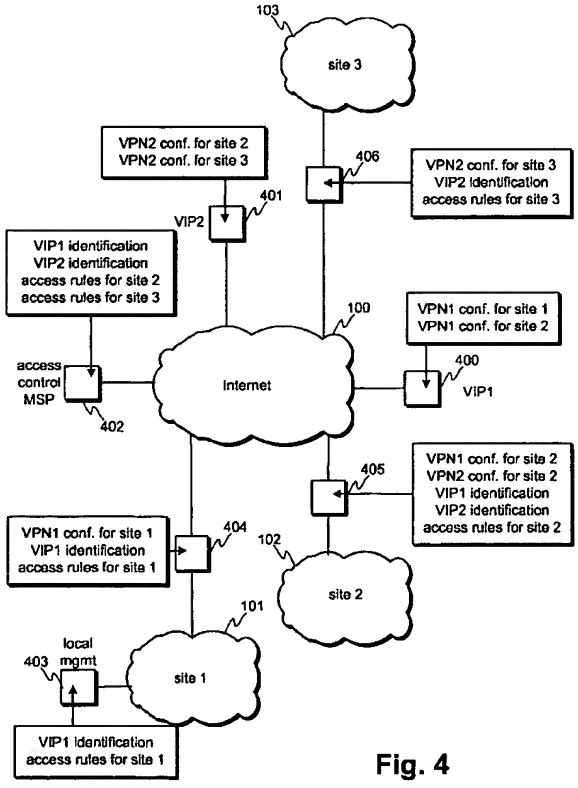

Fig. 4

EP 1 304 830 A2

Description

BACKGROUND OF THE INVENTION

[0001] The invention relates in general to Virtual Private Networks (VPN). In particular the invention relates to managing VPNs.

[0002] Public networks are presently being used more and more for sensitive and mission critical communications and the internal networks of various organisations and enterprises are nowadays connected to the public networks, Internet being one of them. Since the basic mechanisms of the public networks were originally not designed with secrecy and confidentiality in mind, public networks are untrusted networks.

[0003] Virtual Private Networks (VPN) are commonly used for connecting trusted parties to each other over untrusted public network through a secure tunnel. All traffic from a first party to a second party is encrypted in a security gateway of the first party, sent in encrypted form over the public network to the second party, where the transmitted data is decrypted in a security gateway and the decrypted data is forwarded to the recipient. The VPN is typically transparent to the processes that are communicating between each other and the encryption and decryption depend on the configuration of the VPN between the parties. However, the security gateways need to have information about the configuration of the other end of the VPN in order to be able to encrypt and decrypt the traffic correctly. The configuration includes things like addressing, encryption algorithm and key information of the other end security gateway. The configuration information is usually conveyed between the administrators of different sites by means of phone or some other traditional communication system. The administrators then input the configuration to the security gateways of their sites in order to enable VPN connections between the sites. The actual encryption keys are exchanged in VPN communication, but the configuration that is needed for initiating VPN connection needs to be conveyed by some other means.

[0004] Large VPNs are complicated and tedious to manage. Keeping the information about the structure of the VPN up to date at each site (network or group of networks connected to the VPN) is problematic but mandatory. Every site must have the correct configuration for all the other sites in order to communicate with them. In large VPNs there may be dozens or hundreds of sites and the configuration may vary in time rather frequently, and if the configuration of one VPN site changes all sites need to be updated. That is, the administrator of the sites changing its configuration needs to contact administrators of all other sites and communicate the changes to them, whereby they need to re-configure their security gateways.

[0005] Figure 1 illustrates an example network topology with four sites 101-104, who are able to communicate with each other by means of VPNs. The sites 101-104 are connected to the Internet 100 via security gateways 105-108. Each security gateway is managed via a site-specific management server 109-112, which usually resides inside respective site and to each site there is configured VPN configuration information of all other sites as well as the configuration of the site itself. In case the security gateway functions as a firewall; the firewall configuration (access rules) of the security gateways is naturally not duplicated to the other sites.

[0006] One proposal for managing large VPNs is a star like VPN, where a central "hub" acts as a VPN router. Each site connects to the hub, which decrypts the packets and then re-encrypts them for the connection from the hub to the target site. This way, the VPN sites do not need to have up-to-date VPN information of all other sites; instead it is enough to be able to connect to the central hub.

[0007] Figure 2 illustrates the network topology of Figure 1 in connection with the star like VPN. The sites include now only VPN configuration of the site itself and of a central hub 200. The central hub includes VPN configuration of all the sites in the configuration, and the sites connect to each other via the central hub.

[0008] The disadvantage of the star like VPN is that vast amounts of processing power are required at the hub. The security gateway at each site still has the same amount of encryption load as in a standard distributed VPN, but the hub's load is in fact equal to the sum of the loads of all the sites. In large-scale VPNs this may be difficult or impossible to achieve and in any case very expensive. Furthermore, the data transmitted in the VPNs is in cleartext form within the hub, which is clearly a security risk.

[0009] If all the sites belonging to a VPN belong to the same organization, it is possible to administer them centrally by means of existing tools. In this case, all aspects of the security gateways, including access control configuration, are managed from one central point. However, the sites joining a VPN are not always sites of one party, but many different organizations may wish to establish a VPN between them. Clearly, such central management of all aspects of security gateways is not suitable, if different organizations are involved. Therefore a new way to manage VPNs of more than one organisation and especially large VPNs is required.

SUMMARY OF THE INVENTION

[0010] An object of the invention is to provide a method for managing VPN devices, which avoids or alleviates the problems mentioned above. The object is achieved according to the invention as disclosed in the attached independent claims. Preferred embodiments of the invention are disclosed in the dependent claims. The features described in one dependent claim may be further combined with features described in another dependent claim to produce further embodiments of the invention.

[0011] The idea of the invention is to provide a centralized VPN management of a plurality of VPN sites by means of a VPN Information Provider (VIP). The security gateway (or other VPN device) management is distributed so that at least part of the VPN configuration (especially the part consisting of site addressing, used encryption algorithms and key management) is centrally managed without giving away control of the firewall rulebase or other critical local configuration used in the security gateway. There may be several VPNs handled by different VIPs, so that an organization using the invention can flexibly join several independent VPNs.

[0012] The VIP according to the invention is a mutually trusted party, from which the parties joining a VPN are willing to accept configuration information.

[0013] According to a first aspect of the invention a method for managing VPN devices comprises

- maintaining in a VPN Information Provider (VIP) VPN configurations of VPN devices belonging to a first VPN,
- providing from the VIP to a first VPN device belonging to the first VPN, VPN configuration of at least one other VPN device belonging to the first VPN, and
- managing certain aspects of said first VPN device belonging to the first VPN from at least one other management system.

[0014] According to a second aspect of the invention a method for managing VPN device comprises

- maintaining in a first VPN Information Provider (VIP) VPN configurations of VPN device belonging to a first VPN,
- maintaining in a second VPN Information Provider (VIP) VPN configurations of VPN device belonging to a second VPN, and
- providing to a first VPN device belonging to the first and second VPNs, VPN configuration of at least one other VPN device belonging to the first VPN from the first VIP and VPN configuration of at least one other VPN device belonging to the second VPN from the second VIP.

[0015] The configuration of at least one other VPN device may be provided directly to said first VPN device or via at least one other management system.

[0016] Own VPN configuration of a given VPN device may be defined in the VIP or in some other management system, from where the configuration is provided to the VIP for maintenance.

[0017] Providing the configuration(s) of other VPN devices to a VPN device may be done by sending to a first VPN device belonging to the first VPN, information about the VPN configurations maintained in the VIP, and by requesting from the first VIP VPN configuration of another security gateway belonging to the first VPN when needed. Said information about the VPN configurations maintained in the VIP may be for example a set of addresses included in the first VPN. (The set of addresses may be a single address range or plurality of address ranges related to different sites included in the VPN.) In that case, the request from the first VPN device comprises an address included in the first VPN, and said other VPN device is identified in the VIP by finding a VPN device related to said address. Said information about the configurations - that is, the set of addresses - may be sent to the VPN devices after a change in the set of addresses included in the first VPN, or after a predefined time has elapsed since the information was sent the last time.

[0018] Alternatively the VIP may send, to VPN devices belonging to the first VPN, VPN configurations maintained in the VIP, so that the configurations are readily available in the VPN devices when needed. The VPN configurations maintained in the VIP may be sent for example after a new VPN configuration has been added to the VIP, after an old VPN configuration has been removed from the VIP, after a VPN configuration of at least one VPN device has been changed in the VIP, or after a predefined time has elapsed since the configurations were sent the last time. That is, all changes need to be instantly conveyed to the VPN devices.

[0019] In either of the above cases, the VIP may send only changes or additions to the information or configurations previously sent (an incremental update) or all available information or configurations (a full update).

[0020] According to a third aspect of the invention a method for handling VPN configuration in a VPN device comprises

- receiving a packet directed to a destination address in a first VPN,
- requesting and receiving VPN configuration for a VPN device related to said destination address from a VPN Information Provider (VIP) administering the first VPN, and
- using said VPN configuration for establishing a VPN tunnel to said VPN device related to said destination address for reaching said destination address.

[0021] In this context, a VPN device related to a destination address refers to the VPN device, which is securing the site, to which the destination address belongs. In order to communicate to the destination address, a VPN tunnel needs to be created to this VPN device.

[0022] According to a fourth aspect of the invention a method for handling VPN configuration in a VPN Information Provider (VIP) comprises

- maintaining VPN configurations of VPN devices belonging to a first VPN,
- providing to VPN devices belonging to the first VPN, information about the VPN configurations main-

tained in the VIP,

- receiving from a first VPN device belonging to the first VPN, a request for VPN configuration of another VPN device belonging to the first VPN, and
- sending to said first VPN device belonging to the first VPN, the VPN configuration of the other VPN device as a response to the request.

[0023] According to the invention all entire encryption/decryption load is addressed to the firewalls or security gateways protecting the sites, while the VPN administration is centralized by means of VIPs to achieve consistent configuration at every site. Also there is no centralized location where all the traffic is in cleartext form as in the central hub arrangement, so the communication is more secure than in a star like structure.

[0024] The method of the invention enables flexible management of a VPN between several autonomous organizations. Additionally, providing VPN management as a service is enabled. That is, the invention offers MSPs (Managed Service Providers) a possibility to provide a new type of service by means of VIPs. VPN configuration is managed separately from other configuration information and therefore management of VPN configuration can be securely outsourced and an organization can easily join different VPNs, which may be administered by a plurality of different VIPs.

[0025] These and other features of the invention, as well as the advantages offered thereby, are described hereinafter with reference to embodiments illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0026]

Figure 1 illustrates an example network topology,
Figure 2 illustrates a star like VPN topology,
Figures 3, 4 and 5 illustrate example network topologies according to the invention,
Figure 6 is a flow chart illustrating management of VPN devices according to an aspect of the invention,
Figure 7 is a flow chart illustrating management of VPN devices according to another aspect of the invention, and
Figure 8 is a flow chart illustrating handling of VPN configuration in a VPN device according to still other aspect of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0027] Figures 1 and 2 are discussed in more detail above in connection with the prior art description.

[0028] In the following description the invention is mainly disclosed in connection with a VPN capable firewall implementation. However, the method of the invention can be applied straightforwardly also in any security gateway without firewall functionality as well as in a VPN client solution, which provides VPN connectivity for a single (and often mobile) host. Additionally, the invention can be used in connection with dynamic security gateway (gateways, which do not have a static IP-address). Therefore, the invention can be employed in any device acting as an endpoint of a VPN.

[0029] According to one aspect of the invention VPN device's own VPN configuration is defined and maintained in a local management system, or in MSP's management system, if the VPN device is administered by an MSP. The VPN configuration may be defined together with access rule configuration of the VPN device, if the VPN device acts as a firewall. However, the VPN device may be only a simple encryption/decryption endpoint of a VPN without firewall functionality. When the site behind the VPN device wants to join for example VPN1, the VPN configuration of the VPN device is provided to VIP1, which is managing VPN1. Alternatively, the VPN configuration may be provided to the gateway from the VIP1.

[0030] VIP1 provides the VPN device with VPN configurations of other endpoints belonging to VPN1 or information about the configuration of the VPN1 as a whole. In the former case, the VPN device uses the configuration normally for communicating over VPN1 and VIP1 takes care of that the configuration, which the VPN device has, is up-to-date. In the latter case, the VPN device queries the actual configuration from the VIP1 when needed.

[0031] It must be appreciated that the arrangement of the invention does not compromise security of the VPNs, even though the VPN configuration information of all sites is available from a central point (VIP). The configuration includes the authentication keys of the sites, that is the end points of the VPNs, but in VPN each connection is encrypted with connection specific keys, which are negotiated between the communicating sites, and thus knowing the authentication key of a site does not enable breaking into a VPN connection.

[0032] Figure 3 illustrates an example network topology according to one aspect of the invention. The sites of the Figure 1 are secured by security gateways 301-304, which include the VPN configuration related to the VPN between the sites for other sites as in prior art. Thus, the security gateways are taking care of all encryption tasks. However, now the local management systems 305-308 do not take care of providing the VPN configuration to the security gateways. VPN configuration information of the sites is loaded to the security gateways from a VPN Information Provider (VIP) 300. It must be noted herein, that even though only one VIP is shown in the Figure, VPN configuration for some other VPN may be loaded to the security gateways from some other VIP, and that the number of different VPN configurations and VIPs used is not restricted.

[0033] When configuration of one site is changed the change needs to be done only in the VIP from which the

updated configuration is then loaded to security gateways of all sites. The VIP loads the configuration to the security gateways for example every time after a change occurs in the configuration. The change may be an addition or removal of a site or modification of some site's configuration. In addition, the VIP may push the configuration information to the security gateways after certain time interval has elapsed since the configuration was pushed the last time in order to minimize the possibility that the sites would not have up-to-date configuration. The security gateways use the VPN configuration loaded from the VIP in the same way, as they would use configuration loaded from a local management system. The security gateways basically need to be configured to accept configuration from the VIP, but otherwise their operation does not need to be altered. The communication between the VIP and the security gateways is encrypted by some suitable means; for example Secure Sockets Layer (SSL) protocol may be used for this. In addition to this some parts of the configuration of the security gateways, e.g. configuration not related to the VPNs, and/or possible access rules related to the VPN are managed from site-specific local management systems 305-308.

[0034] Instead of pushing the whole configuration to the security gateways after every change, the VIP may push only indication that the configuration has changed and the security gateway may initiate the transfer of updated configuration from the VIP to the security gateway.

[0035] Figure 4 illustrates an example network topology according to another aspect of the invention. Here three sites are secured by means of security gateways 404-406, out of which security gateway 404 is managed from a local management 403 and security gateways 405 and 406 are managed from MSP's management system 402. Naturally MSP's management connection to the security gateways 405 and 406 does not need to be over the Internet as shown in the Figure, but can be for example leased line. Security gateways of sites 1 and 2, which join in VPN1, are provided with identification information for VIP1 400 (VIP identification is defined in a local management or in MSPs management system), which is administering VPN1. The sites receive VPN configuration for VPN1 from VIP1. Equally, security gateways of sites 2 and 3, which join in VPN2, are provided with identification information for VIP2 401, which is administering VPN2, and receive VPN configuration for VPN2 from VIP2. Thus, security gateway 405 of site 2 has identification information for both VIP1 and VIP2. When a security gateway detects a packet, which is destined to a host in a VPN the security gateway belongs to, the security gateway queries VPN configuration needed for establishing a VPN tunnel for reaching the host.

[0036] In this scenario, all VPN configurations are not distributed to the security gateways. Instead, the security gateways query the configuration from the VIP when needed. In order to be able to query configuration, the security gateways need to know from which VIP to query it. For this purpose, the VIPs send to security gateways information about the configurations they have. This information may be for example a list of IP-addresses included in the VPN or list of VPN sites included in the VPN. In principle this means the addresses, which can be reached over by means of the respective VPN. In the latter case the specific other endpoint (other VPN device and its configuration) to which a certain VPN tunnel should be destined is provided to a security gateway only when needed. The benefit of this solution is that smaller amount of data needs to be distributed to the security gateways. Since it is likely that in many VPN's all gateways do not communicate with all other gateways, all gateways do not necessarily need configuration for all possible other endpoints. Moreover, only fundamental changes in the configuration of the whole VPN trigger the need to distribute data to all security gateways. Since configuration of a gateway is queried from the VIP before use, minor changes in configuration of one security gateway do not need to be immediately communicated to all other security gateways. Only if a new site is added or removed from the VPN, i.e. the address range of the VPN changes, all security gateways need to be informed of the change.

[0037] In addition, this arrangement enables the use of dynamic security gateways. If a security gateway obtains its address dynamically, for example from a DHCP (Dynamic Host Configuration Protocol) server, other gateways cannot know from which address the dynamic security gateway is reached at a given time. Now, addresses behind the dynamic security gateway can be maintained in a VIP and conveyed to other gateways from there. Then the dynamic security gateway informs the VIP of its current address every time its address changes. The VIP then conveys the current address to another gateway when needed (other gateways query the current address on the basis of an address included in the site of the dynamic gateway). Since the address of a dynamic gateway may change at any given time, e. g. due to connectivity failures, and other gateways may cache configurations received from a VIP for future use, there is a possibility that a security gateway has an out-of-date configuration for a dynamic gateway. Therefore, it is beneficial that the VIP tags the configuration of a dynamic security gateway differently from static configurations. In this way, a security gateway can for example adjust the time a configuration of a dynamic gateway is cached or otherwise treat dynamic and static entries differently.

[0038] Figure 5 illustrates an example network topology according to still other aspect of the invention. Therein security gateways 503 and 506 of sites 1 and 3 are managed by local management 504 and MSP 502, respectively. VPN configurations of the security gateways defined in the local management or MSP. The configurations are provided to a VIP 500 and maintained

therein. It should be noted herein that when the VIP receives VPN configuration of a security gateway, it could check if the configuration is compatible with VPN policy of the VIP and with VPN configurations of the other security gateways belonging to the VPN. This can be done by simply comparing the new configuration to configurations of other gateways. When the security gateways are establishing a VPN tunnel they first query the configuration of the other endpoint from the VIP. (This is described in more detail above in connection with Figure 4.)

[0039] In addition to the sites 1 and 3 belonging to the VPN, there is a VPN client 505 joining in the VPN as well. The VPN configuration of the VPN client is maintained in the VIP in similar way as the configurations of the dynamic security gateways.

[0040] The example implementations of the invention illustrated in Figures 3 to 5 are not meant to be restrictive. Instead, implementation details related to one example may be combined to the details of another example in any suitable way.

[0041] The VIP and the VPN devices (security gateways, firewalls, VPN clients) according to the invention may be implemented as a suitable combination of hardware and software. Typically the implementation is software program code executed in a processor unit combined with suitable memory resources.

[0042] A major part of the implementation of the invention is a change in the handling of the configuration in the VPN device. A VPN device according to the invention is adapted to receive configuration from more than one management entity, e.g. from a local management and a VIP. In general VIP provides VPN configuration and local management provides access rule configuration. However, local management may provide VPN configuration as well. The VPN device is adapted to identify different VIP for example by means of certificates. In addition, VPN device may check, if a VPN configuration received from a VIP is in accordance with other configuration of the VPN device, before accepting the configuration for use.

[0043] A VIP can be basically similar to a centralized VPN management system able to handle VPN devices; the VIP includes thus capability to define VPN configurations and to upload them to the VPN devices. Alternatively, a VIP may accept readily defined VPN configurations for maintenance. In this case the VIP administering a VPN is preferably adapted to confirm that a received new configuration is compatible with the configurations of other gateways belonging to the VPN. In addition a VIP according to one aspect of the invention comprises mechanism for providing VPN devices with information about the configurations maintained in the VIP and sending configuration to VPN devices on demand, that is, as a response to a request.

[0044] Features of the invention are further illustrated in the flow charts of Figures 6, 7 and 8. Figure 6 is a flow chart illustrating management of VPN devices according to an aspect of the invention. In steps 600 and 602, VPN configurations are defined for VPN devices and the configurations are maintained in a VIP. The VPN configuration of a given VPN device may be defined in the VIP or in some other management system, from where the configuration is provided to the VIP for maintenance. Then in step 604, a VPN device is provided with VPN configuration of some other VPN device by means of sending the configuration from the VIP. In step 606 certain aspects of the VPN devices are managed from some other management system. Such aspects may be for example access rule configurations or configurations related to some other VPN configuration.

[0045] Figure 7 is a flow chart illustrating management of VPN devices according to another aspect of the invention. Therein, VPN configurations are defined for VPN devices belonging to first and second VPNs in step 700. The configurations for the first VPN are maintained in a first VIP and the configurations for the second VPN are maintained in a second VIP in steps 702 and 704 respectively. Also in this case the VPN configuration of a given VPN device may be defined in a VIP or in some other management system, from where the configuration is provided to the respective VIP for maintenance. Then in step 706, a VPN device belonging to the first and second VPNs obtains VPN configuration of at least one other VPN device belonging to the first VPN from the first VIP and VPN configuration of at least one other VPN device belonging to the second VPN from the second VIP.

[0046] Figure 8 is a flow chart illustrating handling of VPN configuration in a VPN device according to still other aspect of the invention. In step 800, the VPN device receives information about the VPN configurations maintained in a VIP (e.g. set of addresses included in the respective VPN). Then the VPN device receives a data packet destined to the VPN in step 802. On the basis of the information received from the VIP the VPN device queries VPN configuration from the VIP in step 804 and uses VPN configuration obtained from the VIP for establishing a VPN tunnel for the data packet.

[0047] It will be apparent for those skilled in the art that the illustrative embodiments described are only examples and that various modifications can be made within the scope of the invention as defined in the appended claims.

Claims

1. A method for managing VPN devices, **characterized in that** the method comprises the steps of

   - maintaining (602) in a VPN Information Provider (VIP) VPN configurations of VPN devices belonging to a first VPN,
   - providing (604) from the VIP to a first VPN device belonging to the first VPN, VPN configura-

tion of at least one other VPN device belonging to the first VPN, and
- managing (606) certain aspects of said first VPN device belonging to the first VPN from at least one other management system.

2. A method as claimed in claim 1, **characterized in that** said configuration of at least one other VPN device is provided to said first VPN device via said at least one other management system.

3. A method as claimed in claim 1, **characterized in that** said configuration of at least one other VPN device is provided directly to said first VPN device.

4. A method as claimed in any one of claims 1 to 3, **characterized by** further comprising

- defining (600) said VPN configurations of said VPN devices belonging to the first VPN in said at least one other management system, and
- providing said VPN configurations to the VIP for maintenance.

5. A method as claimed in any one of claims 1 to 3, **characterized by** further comprising

- defining (600) said VPN configurations of said VPN devices belonging to the first VPN in the VIP, and
- providing said VPN configurations to respective VPN devices.

6. A method as claimed in any one of claims 1 to 5, **characterized in that** the step of providing comprises

- sending to VPN devices belonging to the first VPN, information about the VPN configurations maintained in the VIP,
- receiving from a first VPN device belonging to the first VPN, a request for VPN configuration of another VPN device belonging to the first VPN, and
- sending to said first VPN device belonging to the first VPN, the VPN configuration of the other VPN device as a response to the request.

7. A method as claimed in claim 6, **characterized in that** said information about the VPN configurations maintained in the VIP is a set of addresses included in the first VPN, said request from the first VPN device comprises an address included in the first VPN, and said other VPN device is identified in the VIP by finding a VPN device related to said address.

8. A method as claimed in claim 6, **characterized in that** said information about the VPN configurations maintained in the VIP is a set of addresses included in the first VPN, and said information is sent after a change in the set of addresses included in the first VPN, or after a predefined time has elapsed since the information was sent the last time.

9. A method as claimed in any one of claims 1 to 5, **characterized in that** the step of providing comprises

- sending to VPN devices belonging to the first VPN, VPN configurations maintained in the VIP.

10. A method as claimed in claim 9, **characterized in that** said VPN configurations maintained in the VIP are sent after a new VPN configuration has been added to the VIP, after an old VPN configuration has been removed from the VIP, after a VPN configuration of at least one VPN device has been changed in the VIP, or after a predefined time has elapsed since the configurations were sent the last time.

11. A method for managing VPN devices, **characterized in that** the method comprises the steps of

- maintaining (702) in a first VPN Information Provider (VIP) VPN configurations of VPN devices belonging to a first VPN,
- maintaining (704) in a second VPN Information Provider (VIP) VPN configurations of VPN devices belonging to a second VPN, and
- providing (706) to a first VPN device belonging to the first and second VPNs, VPN configuration of at least one other VPN device belonging to the first VPN from the first VIP and VPN configuration of at least one other VPN device belonging to the second VPN from the second VIP.

12. A method as claimed in claim 11, **characterized in that** said configuration of at least one other VPN device is provided to said first VPN device via at least one other management system.

13. A method as claimed in claim 11, **characterized in that** said configuration of at least one other VPN device is provided directly to said first VPN device.

14. A method as claimed in any one of claims 11 to 13, **characterized by** further comprising

- defining (700) said VPN configurations of said VPN devices belonging to the first and second VPNs in at least one other management system, and
- providing said VPN configurations to the VIPs for maintenance.

15. A method as claimed in any one of claims 11 to 13, **characterized by** further comprising

- defining (700) said VPN configurations of said VPN devices belonging to the first VPN in the first VIP and said VPN configurations of said VPN devices belonging to the second VPN in the second VIP, and
- providing said VPN configurations to respective VPN devices.

16. A method as claimed in any one of claims 11 to 15, **characterized in that** the step of providing comprises

- sending to VPN devices belonging to a VPN, information about the VPN configurations maintained in the respective VIP,
- receiving from a first VPN device belonging to the VPN, a request for VPN configuration of another VPN device belonging to the VPN, and
- sending to said first VPN device belonging to the VPN, the VPN configuration of the other VPN device as a response to the request.

17. A method as claimed in claim 16, **characterized in that** said information about the VPN configurations maintained in the VIP is a set of addresses included in the first VPN, said request from the first VPN device comprises an address included in the first VPN, and said other VPN device is identified in the VIP by finding a VPN device related to said address.

18. A method as claimed in claim 16, **characterized in that** said information about the VPN configurations maintained in the VIP is a set of addresses included in the first VPN, and said information is sent after a change in the set of addresses included in the first VPN, or after a predefined time has elapsed since the information was sent the last time.

19. A method as claimed in any one of claims 11 to 15, **characterized in that** the step of providing comprises

- sending to VPN devices belonging to a VPN, VPN configurations maintained in the respective VIP.

20. A method as claimed in claim 19, **characterized in that** said VPN configurations maintained in the VIP are sent after a new VPN configuration has been added to the VIP, after an old VPN configuration has been removed from the VIP, after a VPN configuration of at least one VPN device has been changed in the VIP, or after a predefined time has elapsed since the configurations were sent the last time.

21. A method for handling VPN configuration in a VPN device, the method comprising

- receiving (802) a packet directed to a destination address in a first VPN, the method being **characterized by**
- requesting and receiving (804) VPN configuration for a VPN device related to said address from a VPN Information Provider (VIP) administering the first VPN, and
- using (806) said VPN configuration for establishing a VPN tunnel to said VPN device related to said destination address for reaching said destination address.

22. A method for handling VPN configuration in a VPN Information Provider (VIP), **characterized in that** the method comprises

- maintaining VPN configurations of VPN devices belonging to a first VPN,
- providing to VPN devices belonging to the first VPN, information about the VPN configurations maintained in the VIP,
- receiving from a first VPN device belonging to the first VPN, a request for VPN configuration of another VPN device belonging to the first VPN, and
- sending to said first VPN device belonging to the first VPN, the VPN configuration of the other VPN device as a response to the request.

23. An arrangement for managing VPN devices comprising

- at least two VPN devices (301-304, 404, 405, 503, 505, 506) belonging to a first VPN, the arrangement being **characterized by** comprising
- a VPN Information Provider (VIP) (300, 400, 500) maintaining VPN configurations of VPN devices belonging to the first VPN, and
- at least one other management system (305-308, 402, 403, 502, 504) managing certain aspects of said VPN devices belonging to the first VPN, while

the VPN devices are adapted to receive from the at least one other management system, a first part of configuration, and from the VIP, a second part of configuration, which comprises VPN configuration of at least one other VPN device belonging to the first VPN.

24. An arrangement as claimed in claim 23, **characterized in that** the first part of configuration comprises VPN configuration and /or access rule configuration.

25. An arrangement for managing VPN devices, **characterized by** comprising

- at least two VPN Information Providers (VIP), a first one (400) maintaining VPN configurations of VPN devices belonging to a first VPN and a second one (401) maintaining VPN configurations of VPN devices belonging to a second VPN, and
- a VPN device (405) belonging to the first and second VPNs and receiving VPN configuration information from the first and second VIPs.

26. A VPN device (301-304, 404, 405, 503, 505, 506) comprising

- a mechanism for receiving a packet directed to a destination address in a first VPN, the VPN device being **characterized by** comprising
- mechanisms for requesting and receiving VPN configuration for a VPN device related to said address from a VPN Information Provider (VIP) administering the first VPN, and
- a mechanism for using said VPN configuration for establishing a VPN tunnel to said VPN device related to said destination address for reaching said destination address..

27. A VPN Information Provider (VIP) (300, 400, 401, 500) **characterized by** comprising

- a mechanism for maintaining VPN configurations of VPN devices belonging to a first VPN,
- a mechanism for providing to VPN devices belonging to the first VPN, information about the VPN configurations maintained in the VIP,
- a mechanism for receiving from a first VPN device belonging to the first VPN, a request for VPN configuration of another VPN device belonging to the first VPN, and
- a mechanism for sending to said first VPN device belonging to the first VPN, the VPN configuration of the other VPN device as a response to the request.

28. A computer-readable medium, comprising program code which, when executed on a computer device, causes the computer device to provide a VPN device functionality comprising

- receiving a packet directed to a destination address in a first VPN, - requesting and receiving VPN configuration for a VPN device related to said addressfrom a VPN Information Provider (VIP) administering the first VPN, and
- using said VPN configuration for establishing a VPN tunnel to said VPN device related to said destination address for reaching said destination address.

29. A computer-readable medium comprising program code which, when executed on a computer device, causes the computer device to provide a VPN Information Provider (VIP) functionality comprising

- maintaining VPN configurations of VPN devices belonging to a first VPN,
- providing to VPN devices belonging to the first VPN, information about the VPN configurations maintained in the VIP,
- receiving from a first VPN device belonging to the first VPN, a request for VPN configuration of another VPN device belonging to the first VPN, and
- sending to said first VPN device belonging to the first VPN, the VPN configuration of the other VPN device as a response to the request.

30. A computer program code which, when executed on a computer device, causes the computer device to provide a VPN device functionality comprising

- receiving a packet directed to a destination address in a first VPN,
- requesting and receiving VPN configuration for a VPN device related to said address from a VPN Information Provider (VIP) administering the first VPN, and
- using said VPN configuration for establishing a VPN tunnel to said VPN device related to said destination address for reaching said destination address.

31. A computer program code which, when executed on a computer device, causes the computer device to provide a VPN Information Provider (VIP) functionality comprising

- maintaining VPN configurations of VPN devices belonging to a first VPN,
- providing to VPN devices belonging to the first VPN, information about the VPN configurations maintained in the VIP,
- receiving from a first VPN device belonging to the first VPN, a request for VPN configuration of another VPN device belonging to the first VPN, and
- sending to said first VPN device belonging to the first VPN, the VPN configuration of the other VPN device as a response to the request.

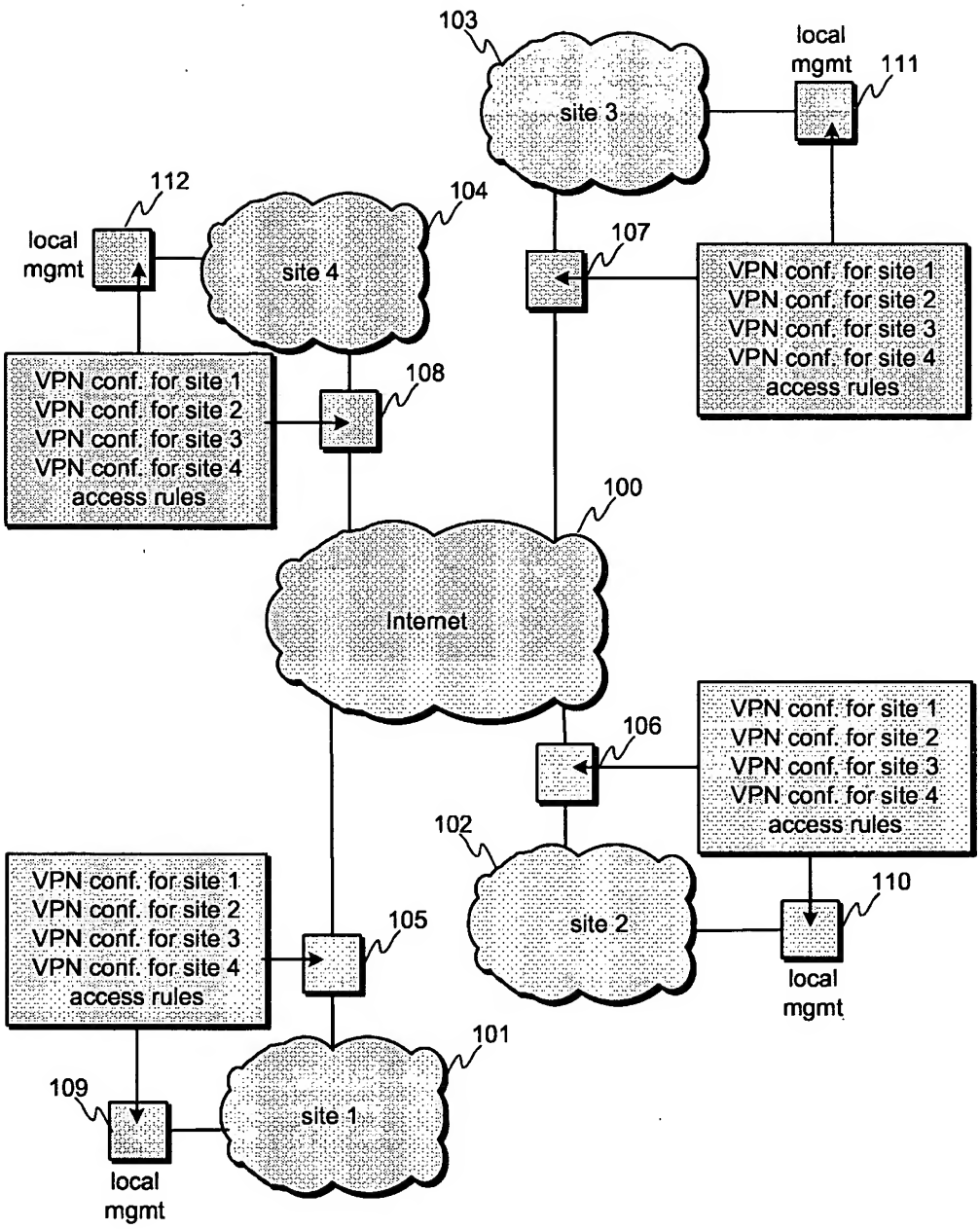
103
site 3
local
mgmt
111
112
local
mgmt
104
site 4
107
VPN conf. for site 1
VPN conf. for site 2
VPN conf. for site 3
VPN conf. for site 4
access rules
VPN conf. for site 1
VPN conf. for site 2
VPN conf. for site 3
VPN conf. for site 4
access rules
108
100
Internet
VPN conf. for site 1
VPN conf. for site 2
VPN conf. for site 3
VPN conf. for site 4
access rules
106
102
site 2
110
local
mgmt
VPN conf. for site 1
VPN conf. for site 2
VPN conf. for site 3
VPN conf. for site 4
access rules
105
101
109
site 1
local
mgmt

Fig. 1

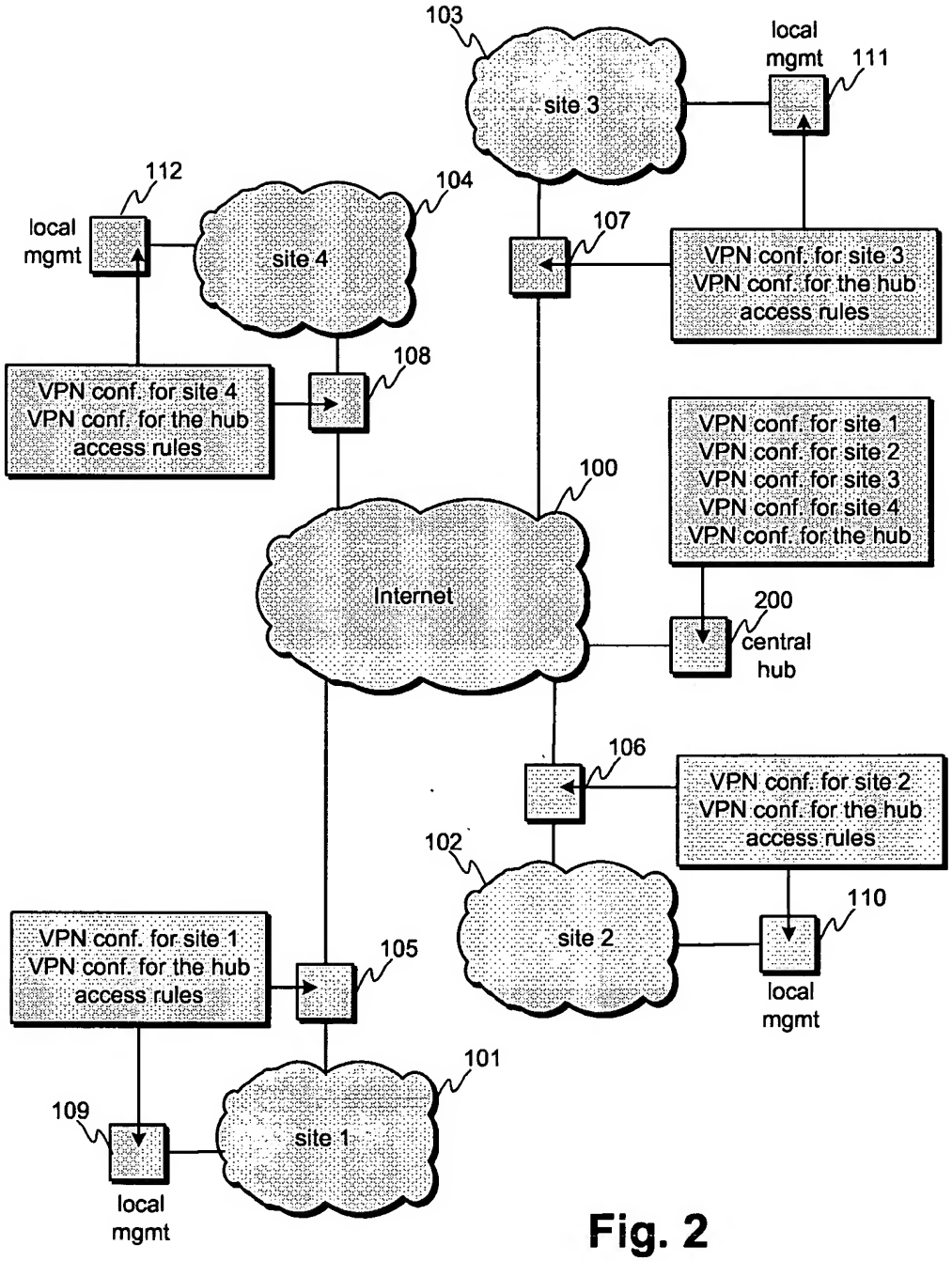
103
site 3
local mgmt
111
112
local mgmt
104
site 4
107
VPN conf. for site 3
VPN conf. for the hub
access rules
108
VPN conf. for site 4
VPN conf. for the hub
access rules
VPN conf. for site 1
VPN conf. for site 2
VPN conf. for site 3
VPN conf. for site 4
VPN conf. for the hub
100
Internet
200
central hub
106
VPN conf. for site 2
VPN conf. for the hub
access rules
102
site 2
110
local mgmt
VPN conf. for site 1
VPN conf. for the hub
access rules
105
101
109
site 1
local mgmt

Fig. 2

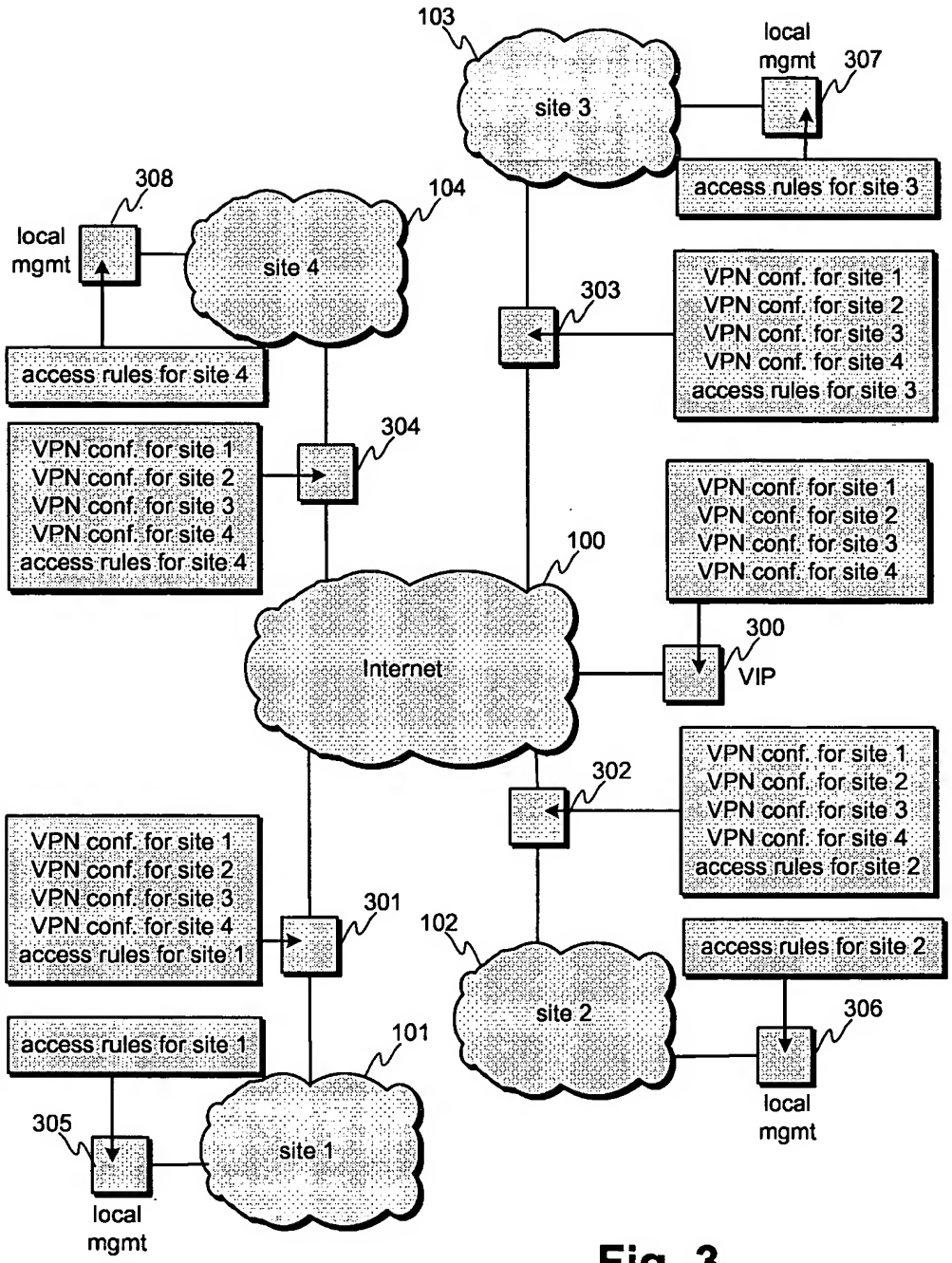
103
site 3
local mgmt
307
access rules for site 3
308
local mgmt
104
site 4
access rules for site 4
303
VPN conf. for site 1
VPN conf. for site 2
VPN conf. for site 3
VPN conf. for site 4
access rules for site 3
304
VPN conf. for site 1
VPN conf. for site 2
VPN conf. for site 3
VPN conf. for site 4
access rules for site 4
100
Internet
VPN conf. for site 1
VPN conf. for site 2
VPN conf. for site 3
VPN conf. for site 4
300
VIP
302
VPN conf. for site 1
VPN conf. for site 2
VPN conf. for site 3
VPN conf. for site 4
access rules for site 2
VPN conf. for site 1
VPN conf. for site 2
VPN conf. for site 3
VPN conf. for site 4
access rules for site 1
301
102
site 2
access rules for site 2
306
local mgmt
access rules for site 1
101
305
site 1
local mgmt

Fig. 3

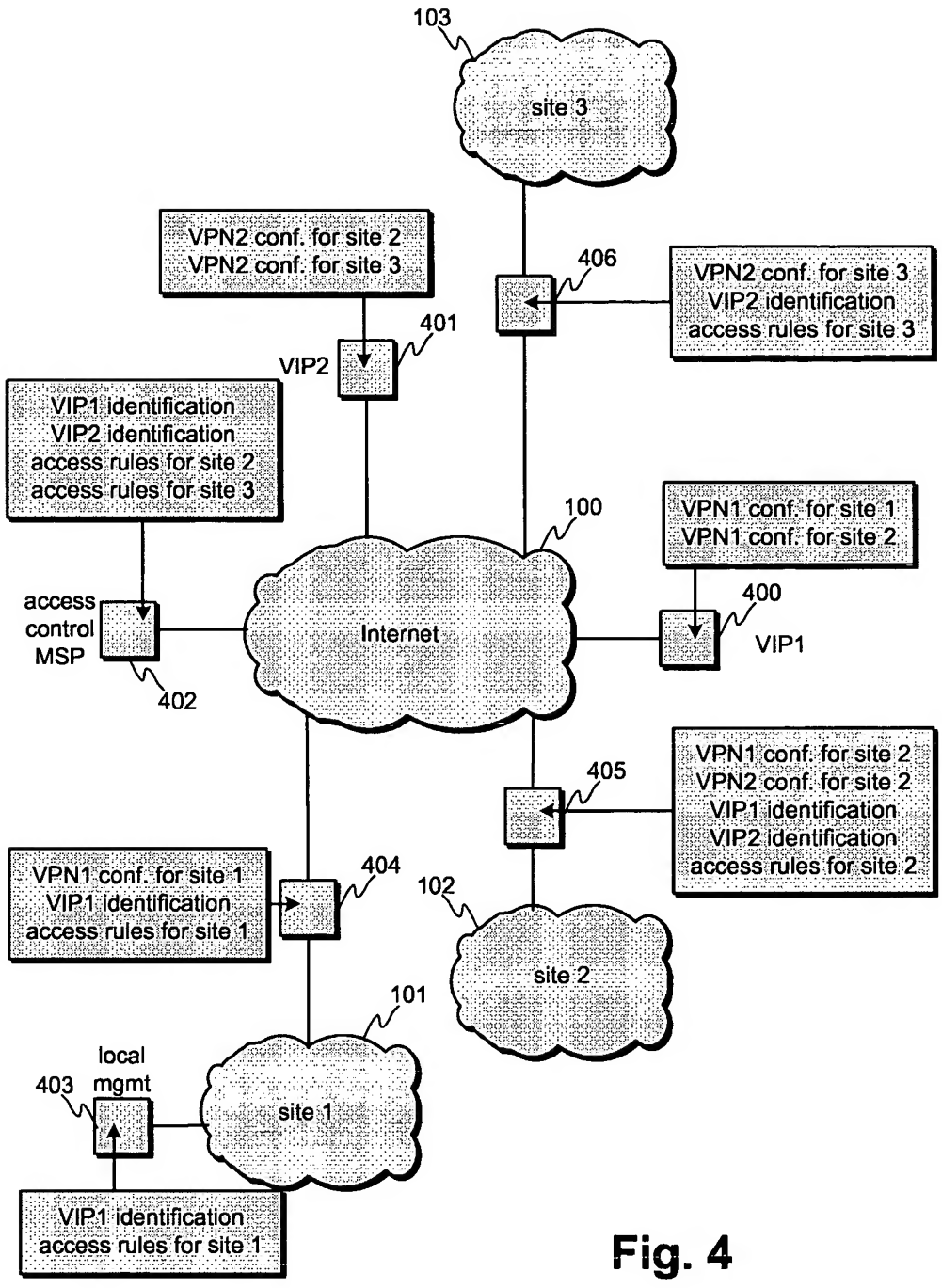
103
site 3
VPN2 conf. for site 2
VPN2 conf. for site 3
406
VPN2 conf. for site 3
VIP2 identification
access rules for site 3
401
VIP2
VIP1 identification
VIP2 identification
access rules for site 2
access rules for site 3
100
VPN1 conf. for site 1
VPN1 conf. for site 2
400
VIP1
access
control
MSP
Internet
402
VPN1 conf. for site 2
VPN2 conf. for site 2
VIP1 identification
VIP2 identification
access rules for site 2
405
VPN1 conf. for site 1
VIP1 identification
access rules for site 1
404
102
site 2
101
local
mgmt
403
site 1
VIP1 identification
access rules for site 1

Fig. 4

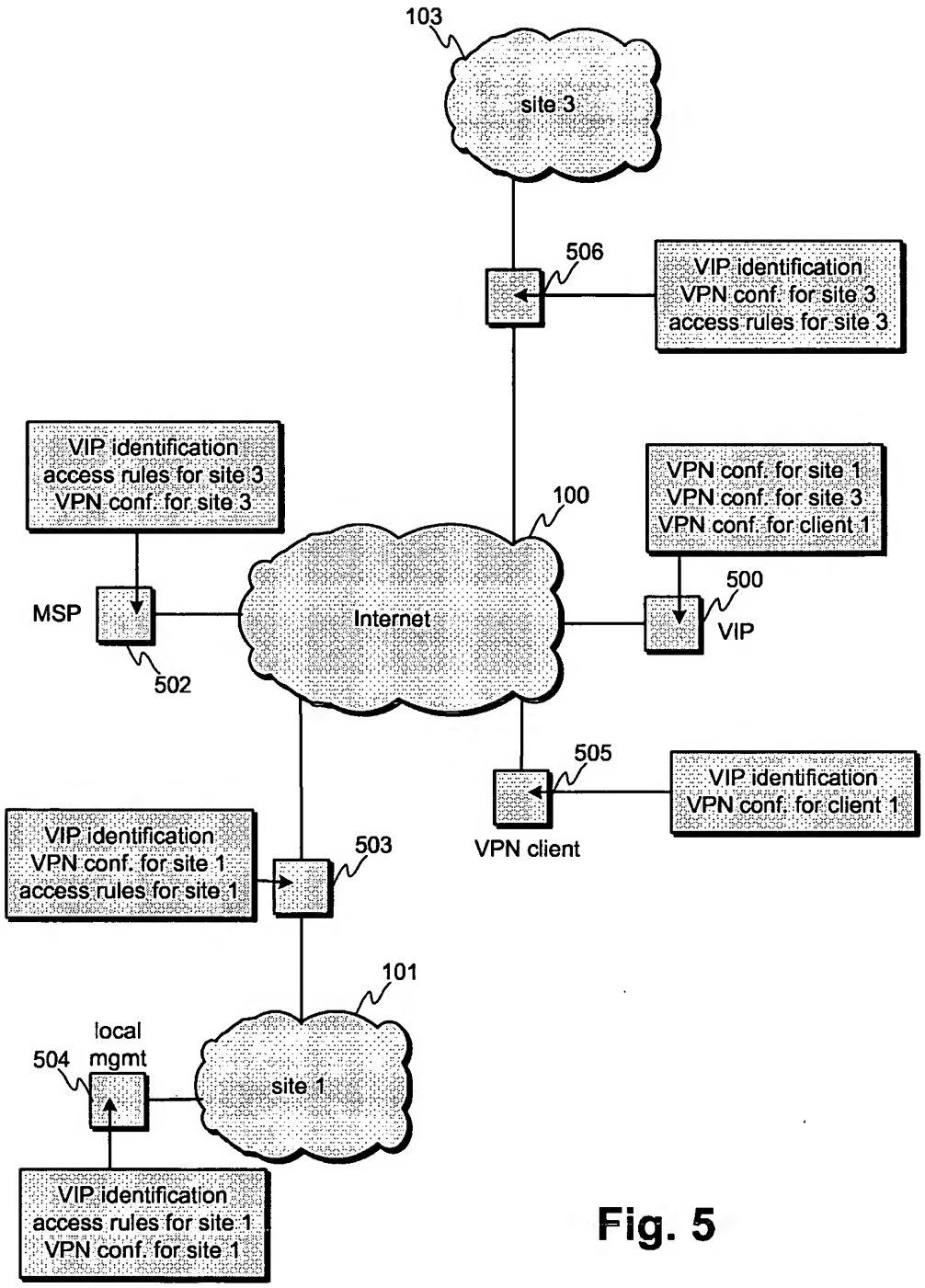
103
site 3
506
VIP identification
VPN conf. for site 3
access rules for site 3
VIP identification
access rules for site 3
VPN conf. for site 3
100
VPN conf. for site 1
VPN conf. for site 3
VPN conf. for client 1
500
VIP
MSP
Internet
502
505
VIP identification
VPN conf. for client 1
VPN client
VIP identification
VPN conf. for site 1
access rules for site 1
503
101
local
mgmt
504
site 1
VIP identification
access rules for site 1
VPN conf. for site 1

Fig. 5

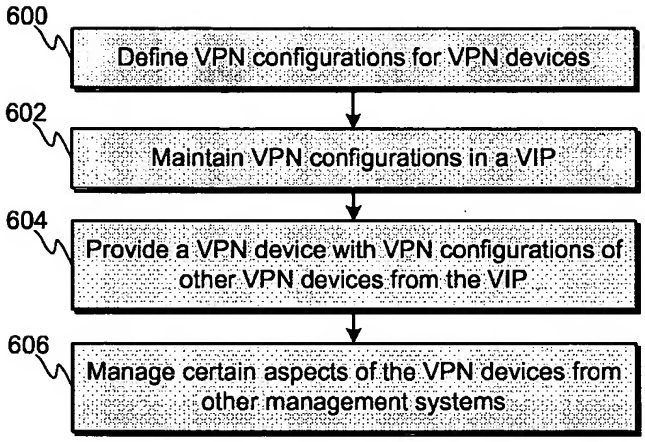

Fig. 6

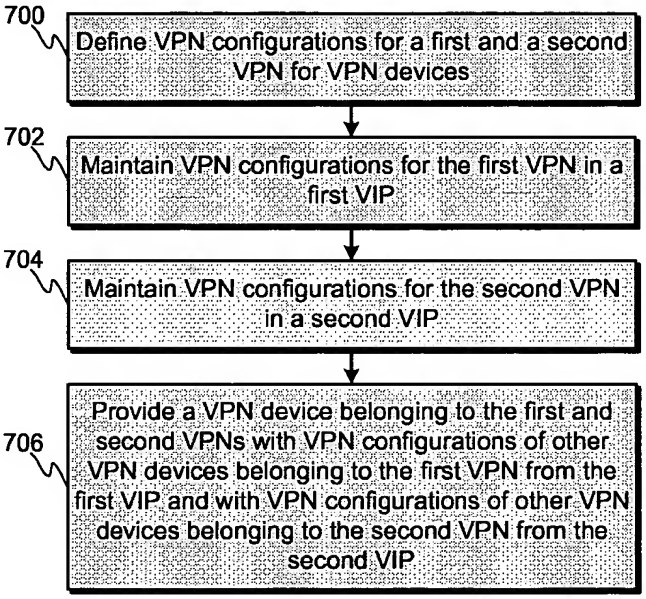

Fig. 7

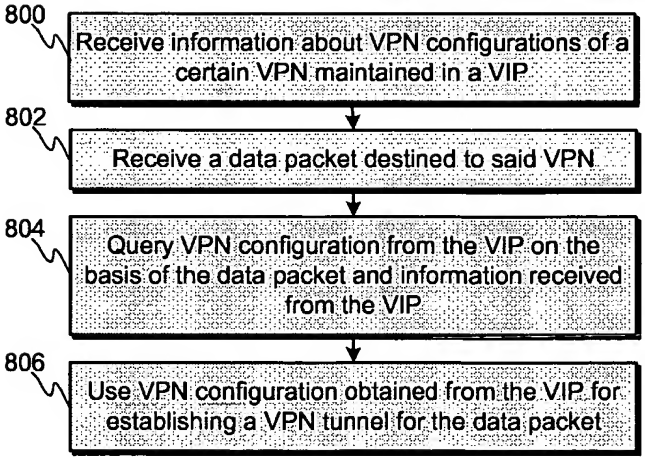

Fig. 8

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 304 830 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
13.08.2003 Bulletin 2003/33

(43) Date of publication A2:
23.04.2003 Bulletin 2003/17

(21) Application number: **02102400.5**

(22) Date of filing: **01.10.2002**

(51) Int Cl.[7]: **H04L 12/24**, H04L 29/06, H04L 12/46

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **05.10.2001 FI 20011949**
21.05.2002 US 151319

(71) Applicant: **Stonesoft Corporation**
00210 Helsinki (FI)

(72) Inventor: **Jalava, Mika**
02580 Siuntio (FI)

(74) Representative: **Äkräs, Tapio**
Kolster Oy Ab,
Iso Roobertinkatu 23
00120 Helsinki (FI)

(54) Virtual private network management

(57) The invention provides a centralized VPN management of a plurality of VPN sites by means of a VPN Information Provider (VIP) (400, 401). Management of a VPN device is distributed so that at least part of the VPN configuration is centrally managed without giving away control of the firewall rulebase or other critical local configuration used in the VPN device.

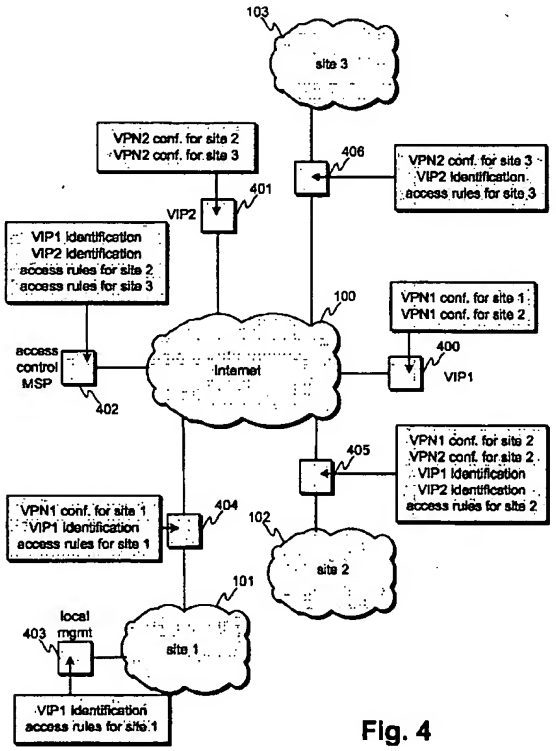

Fig. 4

EP 1 304 830 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 10 2400

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	US 6 079 020 A (LIU QUENTIN C) 20 June 2000 (2000-06-20) * column 2, line 48 - line 49 * * column 6, line 25 - line 36 * * column 7, line 41 - column 8, line 10 * * column 5, line 20 - line 37 * * column 9, line 20 * * column 10, line 26 - line 56 * * figures 4,7-10 * ---	1-35	H04L12/24 H04L29/06 H04L12/46
Y	KOSITPAIBOON R ET AL: "Customer network management for B-ISDN/ATM services" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON COMMUNICATIONS (ICC). GENEVA, MAY 23 - 26, 1993, NEW YORK, IEEE, US, vol. 3, 23 May 1993 (1993-05-23), pages 1-7, XP010136856 ISBN: 0-7803-0950-2 * page 1, right-hand column, line 23 - line 32 * * page 3, right-hand column, line 8 - line 21 * * page 4, right-hand column, line 7 - line 31 * * page 6, left-hand column, line 6 - line 9 * * figures 1,2 * -----	1-35	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
BERLIN	19 May 2003	Siebel, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)